REMARKS

In view of the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application. This amendment is believed to be fully responsive to all issues raised in the 04/26/2004 Office Action.

In the Claims:

Claims 1—19 were originally filed.

Claims 1, 7 and 17 are currently amended.

Claim 2 was canceled.

No claims are added.

Accordingly, claims 1 and 3—19 are pending.

Section 102 Rejection of the Claims

Claims 1, 3, 7, 8 and 17 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,623,637, hereafter "Jones". The Applicants respectfully traverse the rejection and further request that the rejection be reconsidered and withdrawn.

Claim 1 has been amended to recite a system "wherein the memory device stores a user's profile that can be used to configure a computer."

Claim 1 was rejected under §102(b) as being anticipated by Jones. However, the Applicant has amended claim 1 to recite a user's profile that can be used to configure a computer. Due to the amendment, the §102 argument is moot; accordingly the Applicant will address the section 103 argument used in the rejection of claim 2. That argument used the combination of Jones and published application number 20010011341, herein after "Hayes".

Jones teaches use of an encrypted data storage card including a memory area and a smart card. The contents of the memory area are protected, unless the

user can supply an appropriate password. The smart card also has public and private keys that correspond to similar keys on a remote computer (Fig. 3), thereby allowing secure communication between the host computer to which the secure card (smart card plus memory) is attached and the remote computer.

Hayes teaches a *centralized* method by which user profiles may be maintained by a server, and distributed to clients upon password approval. Therefore, Hayes teaches the centralization of data; accordingly, in promoting the centralized server-client model of data storage, Hayes teaches away from the storage of data on personally possessed portable memory devices. Such personal and portable data storage is inconsistent with the network administrator-controlled model disclosed by Hayes. A passage in Hayes at page 1, paragraph 4, discloses that "an administrator" creates user profiles stored on "a network server". Thus, we see that Hayes teaches away from an environment wherein the user has access to the user's own profile on a memory device "to configure a computer" (claim 1). In fact, Hayes teaches a client-server environment, wherein a user's profile is not even stored on the user's own (client) computer, but are in fact stored remotely, on the network server. Thus, Hayes teaches *centralization*, by putting the client's profiles in a central location, not on their own computer. In contrast, claim 1 recites structures consistent with *decentralization*, wherein the user's data is stored on the memory device which can be "removably" connected a computer, thereby allowing later connection to another computer. Thus, Hayes facilitates an environment wherein everyone's user profile is centrally located; the Applicant's claims recite an environment wherein everyone's profile is not only stored in a distributed manner (locally) but is stored in a manner which allows physical portability of the user profile data.

It would not have been obvious, and there is no motivation, to combine Hayes and Jones. Hayes teaches the use of the network to set up the user's profile and desktop (0011). In contrast, Jones teaches a portable memory device. Since Hayes teaches the use of a network wherein a systems administrator can control and manage user's profile data, there is nothing to motivate Hayes to discard his system and instead to try to adapt Jones' teachings of a portable memory device. Similarly, Jones does not suggest any motivation for utilizing his data storage device for carrying user's profiles. Indeed, there are millions of uses for data storage; nothing in Jones suggests the storage of profile data similar to that which Hayes transfers over a network.

Jones and Hayes teach away from each other; in particular, they disclose different data transfer strategies. They each have benefits, and there is no reason to expect that either would be motivated to adopt the strategy of the other. In particular:

> Hayes uses a network to distribute data in part because if frees the user of the need to have, maintain or use any type of portable device. Instead, the user simply selects a computer on the network (i.e. a corporate or governmental intranet), provides a password, and receives data which is used to reconfigure the selected computer.
>
> In contrast, Jones teaches use of a portable memory device because it allows transfer of data to any computer configured to accept connection of the portable memory device, regardless of connection to a network. Importantly, nothing in Jones suggests that the data carried on the portable memory device has anything to do with user profiles.

Jones does not suggest the need, benefit or utility of providing or changing a user's profile, access permissions or similar configuration parameters. Jones teaches data storage in a portable device. However, nothing in Jones suggests that there is any benefit in using that device to contain user's profiles.

Similarly, it would not benefit Hayes to so fundamentally change the Hayes invention and teachings (as would be required to follow the decentralized and portable teachings of Jones), given the Hayes goal of using a network to reconfigure computers on the network. Note in paragraph 0011, Hayes discloses that users may "roam" to a new computer, and using the Hayes system to configure (over the network) the new computer to look like their preferred computer. Thus, Hayes teaches the use of a network to move user data, not a portable device, as recited in claim 11. The combination suggested by the Patent Office would essentially "gut" the Hayes invention, by dispensing with the server-client model taught by Hayes.

Claim 3 is allowable due to its dependence on a claim (claim 1) which is allowable for the reasons seen above, as well as for reasons associated with the elements recited by claim 3.

Claim 7 is allowable for reasons substantially similar to those seen above in the discussion of claim 1. In particular, Claim 7 has been amended to recite "user's profiles." User's profiles are not disclosed by Jones. Accordingly, the §102 argument is moot, and the argument seen above with respect to the rejection of claim 1, showing why the combination of Jones and Hayes fails to render the application unpatentable under §103, also applies to claim 7.

Claim 8 is allowable due to its dependence on a claim (claim 7) which is allowable for the reasons seen above, as well as for reasons associated with the elements recited by claim 8.

Claim 17, as amended, recites:

> storing user data and a public key on a portable memory device;
>
> storing a private key on a smart card;
>
> interfacing the smart card and the portable memory device with a computer;
>
> verifying compatibility of the public key and the private key; and
>
> allowing, in response to the verified compatibility, access to the user data on the portable memory device.

Claim 17 is allowable in part because none of the references of record disclose or suggest the step of "verifying compatibility of the public key and the private key" or of "allowing, in response to the verified compatibility, access to the user data on the portable memory device."

Referring in particular to Fig. 3 of the Jones reference, it can be seen that Jones uses public and private keys for the purpose for which they were intended, i.e. the transmission of encrypted messages. In particular, the public key 455 is used by remote computer 450 to send an encrypted message to card 400, which is then decoded with private key 430. Similarly, public key 435 can be used to encrypt a message for transmission from card 400 to remote computer 450, and decoding by private key 460.

Similarly, Sigbjornsen also uses public and private keys for the purpose for which they were intended—in this case encrypting and decrypting computer code.

Fig. 4 of Sigbjornsen clearly shows how (portions of) the source code can be encrypted.

In contrast, the Applicant's claims recite verifying compatibility of the keys, and in response to the verification, allowing access to data. Thus, unlike Jones who uses the keys for transmission of encrypted messages, the Applicant uses the keys—not to send encrypted messages—but to verify compatibility of the smart card and the memory device. Thus, the Applicant uses public key and private key technology not to send an encrypted message, but instead to verify the compatibility of the smart card and the memory device. That is, the public/private key technology is used not for sending messages, but for verifying that the two devices are part of a matched pair.

Claim 17 is additionally allowable for a related reason. Jones does not disclose the use of a public key on the memory device (150, Fig. 2 of Jones). Accordingly, Jones does not verify compatibility of keys on the memory device and on the smart card. Thus, Jones does not verify that the memory device and the smart card are related. By doing so, the Applicant advantageously prevents a user with one smart card from opening a number of memory devices.

Section 103 Rejection of the Claims

Claims 4, 9 and 10 were rejected under §103(a) as being unpatentable over the single Jones reference. The Applicant respectfully traverses the rejection.

Claims 4, 9 and 10 recite "wherein the memory device stores a public key and the smart card stores a corresponding private key and access to the user data in the memory device is enabled upon verification that the public key and the private key are associated" or similar.

Accordingly, claims 4, 9 and 10 are allowable for reasons similar to those seen above, with respect to claim 17. In particular, claims 4, 9 and 10 utilize verification of the compatibility of the public and private keys as a means to verify that the memory device and smart card are both associated with the user and/or each other. This prevents, for example, the user from using her smart card (for which she knows the password) to access someone else's memory device. In contrast, Jones uses public and private key technology to send encrypted messages (the normal use for which such keys were intended).

Additionally, claims 4, 9 and 10 recite storage of a public key in the memory device. In contrast, Jones discloses that the keys are used only in the smart card and a remote host. Thus, Jones fails to disclose the storage, use and operation of a public key in the memory device (e.g. memory device 150 of Fig. 2 of Jones).

Claims 2, 5—6 and 11—16 were rejected under §103(a) as being unpatentable over Jones in view of Hayes. The Applicant respectfully traverses the rejection.

Claim 2 was cancelled.

Claim 5 is allowable for all of the reasons previously discussed with respect to any of the claims in the application. To recap those arguments, it is noted that claim 5 recites the use of user profiles. As seen above, nothing in Jones suggests or discloses the use of a user profile. Jones is concerned with data generally, and makes no suggestion of how user profiles could be utilized. Additionally, Hayes discloses how a network could be utilized to manage user profiles. Accordingly, Hayes teaches centralized administration of the user's profiles under the control of an administrator. Nothing in Hayes suggests that Hayes could decentralize his

system, utilizing portable data carriers. Nothing in the combined Jones and Hayes references discloses how decentralized user profiles on portable memory devices could be implemented.

Additionally, claim 5 recites authentication of "the public key stored on the memory device using the private key." This process confirms that the user, having successfully entered the password for the smart card, has possession of the correct memory device. This is unlike any use of public and private keys in Jones, who uses such keys for their conventional purpose: i.e. sending encrypted messages.

And still further, claim 5 recites having a public key on the memory device, which is not seen in Jones. This allows the Applicant to confirm that the memory device is associated with the smart card, thereby preventing one smart card from opening more than one memory unit. This issue is not addressed by Jones.

Claim 6 is allowable due to its dependence on a claim (claim 5) which is allowable for the reasons seen above, as well as for reasons associated with the elements recited by claim 6. .

Claim 11 is allowable for substantially the same reasons as those discussed with respect to the rejections of claims 1 and 7. In summary, the Jones reference teaches a portable memory device, and Hayes discloses a centralized, networked system wherein user profiles may be downloaded to any computer on the network. Nothing in Jones suggests anything to do with user profiles; moreover, nothing in Hayes suggests the conversion of Hayes' centralized system with control exercised by a network administrator to a decentralized system wherein each user possesses, on a portable device, the user's profile.

Claim 12 is allowable due to its dependence on a claim (claim 11) which is allowable for the reasons seen above, as well as for reasons associated with the elements recited by claim 12.

Claims 13 and 14 recite:

"the IC card stores a first key;

the memory device stores a second key that is associated with the first key; and

the IC card is configured to authenticate the second key passed in from the memory device using the first key as a condition for enabling access to the user's profile"

or similar. Accordingly, claims 13 and 14 are allowable for substantially the same reasons as 4, 9, 10 and 17, as discussed, above.

To summarize these arguments, claims 13 and 14 utilize verification of the compatibility of the public and private keys as a means to verify that the memory device and smart card are both associated with the user and/or associated with each other. This prevents, for example, the user from using her smart card (for which she knows the password) to access someone else's memory device. In contrast, Jones uses public and private key technology to send encrypted messages (the normal use for which such keys were intended).

Additionally, claims 13 and 14 recite storage of a public key in the memory device. In contrast, Jones discloses that the keys are used only in the smart card and a remote host.

Claims 15 and 16 are allowable for substantially the same reasons seen in claims 1, 7 and 11. Those arguments are not reproduced here, in interests of brevity, but are hereby incorporated by reference.

Claims 18 and 19 were rejected under §103(a) as being unpatentable over Jones, in view of Hayes, also in view of U.S. 6,266,416 B1, herein after "Sigbjornsen." The Patent Office cites Sigbjornsen to remedy the deficiencies of Jones and Hayes, and in particular cites a passage in column 7. The Applicant respectfully traverses the rejection.

Claims 18 and 19 are allowable in part because all of the above arguments apply to both of these claims. While the arguments are not reproduced here, they are incorporated by reference. Additional arguments, discussed below, also apply.

Sigbjornsen discloses a software copy/use protection system. As seen in Fig. 2, a portion of the software is protected. In particular, the software may make calls to the smart card (bottom of column 5, top of 6) which can only be handled by a valid smart card. Additionally, a portion of the software, which as been encrypted, is then decrypted by the smart card. See column 7, lines 45—50.

Claim 18 recites in part "authenticating, at the smart card, the device-resident key using the card-resident key" while claim 19 recites in part "authenticating the public key using the private key." Thus, both claims 18 and 19 recite the use of public key/private key technology for verifying the keys are a pair, and by extension, the relationship of the devices from which the keys were obtained is that of a pair of devices. This is in contrast to Sigbjornsen, who utilizes public key/private key technology to encode and decode portions of the code. For example, Figs. 2 and 4 of Sigbjornsen show such use of the keys for encryption; also, at column 7, lines 50—57 it is seen that some portions of the code are encrypted, while leaving other portions unprotected.

Accordingly, Sigbjornsen discloses the use of public key/private key technology for the purpose for which it was designed, i.e. encryption. In contrast,

the Applicant claims "authenticating the public key using the private key," not actually encrypting or decrypting anything, only verifying that the keys, and by extension their respective devices, are compatible (i.e. belong together). This novel use of the public key/private key technology is not shown by Sigbjornsen or other known references.

Conclusion

Claims 1 and 3—19 are in believed to be in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the present application. Should any issue remain that prevents immediate issuance of the application, the Examiner is encouraged to contact the undersigned attorney to discuss the unresolved issue.

Respectfully Submitted,
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

Dated: 7-26-04

By: _____
David S. Thompson
Reg. No. 37,954
Attorney for Applicant

LEE & HAYES PLLC
Suite 500
421 W. Riverside Avenue
Spokane, Washington 99201
Telephone: 509-324-9256 x235
Facsimile: (509) 323-8979